⑲ 日本国特許庁 (JP)　　⑪ 特許出願公開

⑫ 公開特許公報 (A)　　昭58—109970

⑤Int. Cl.³	識別記号	庁内整理番号
G 06 F 15/30		7737—5B
G 07 D 9/00		7536—3E
G 07 F 7/08		7208—3E

⑬公開　昭和58年(1983)6月30日

発明の数　1

審査請求　未請求

(全 13 頁)

⑭不正カードの発行防止方法

⑳特　　願　昭56—215538

㉒出　　願　昭56(1981)12月23日

㉓発 明 者　遠藤侯一　京都市右京区花園土堂町10番地 立石電機株式会社内

㉑出 願 人　立石電機株式会社　京都市右京区花園土堂町10番地

㉔代 理 人　弁理士　小森久夫

明　細　書

1.発明の名称

不正カードの発行防止方法

2.特許請求の範囲

(1) カードの口座番号に対応して、登録暗証番号と、カード発行禁止時にセットされカード発行許可時にリセットされる発行禁止符号と、カード情報登録禁止時にセットされカード情報登録許可時にリセットされる登録禁止符号とを少なくとも含むカード管理情報を記憶する記憶手段、暗証番号入力キーと訂失キーとを有する入力装置、特定のカード発行機、および制御装置を備え、

前記制御装置は、

(A)カードの通常使用時には前記発行禁止符号と前記登録禁止符号とをセットし、

(B)前記暗証番号入力キーと前記訂失キーとが操作されたときには、入力された暗証番号と前記登録暗証番号とが一致した場合だけ前記発行禁止符号をリセットし、

(C)前記発行禁止符号のリセット時に前記カード発行機が動作するとカード発行を許可して、前記登録禁止符号をリセットするとともに前記発行禁止符号をセットし、

(D)前記カード発行機で発行されたカードの初回使用時に前記登録禁止符号がリセットされていれば、カード情報の登録を許可して前記登録禁止符号をセットする、

不正カードの発行防止方法。

3.発明の詳細な説明

この発明は、金融取引処理システム等において使用されるカードが、不正に発行されるのを防止する不正カードの発行防止方法に関する。

キャッシュカード等の磁気カード(以下単にカードという)は、一人の利用者に対して唯一発行されるが、カード使用システムはそのカード利用者が誰であるかを問わないため、カードの使用に対して不正使用の危険が生じる。そこで、一般には一つのカードに対しそのカードの本来の所有者しか知らない暗証番号を対応させ、カード使用のときにその暗証番号の入力を使用条件とさせて個人照

合するようにしている。

一方、カードが紛失したとき等は、カード所有者の要求に応じて、口座　号をもとにして再度カードを発行するようにしている。

しかしながら、このように個人照合をカード再発行時におこなわず、カード使用時にだけおこなう方法では、口座番号が秘密でないためにその番号を利用して不正なカードが作成される恐れがある。

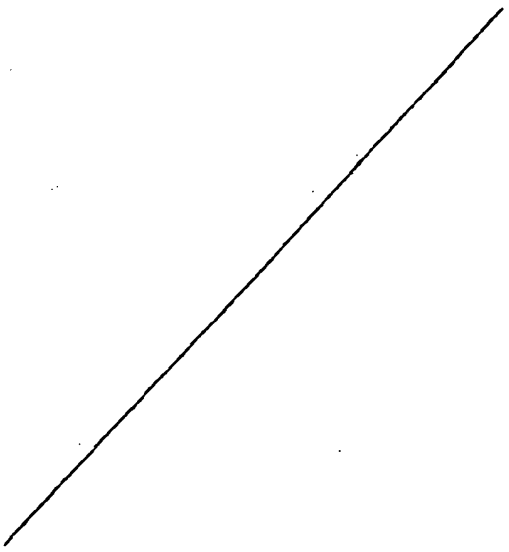
この発明の目的は以上の欠点を解消することにある。

この発明は、要約すれば、

通常時にカードの複数枚発行を禁止する一方、カードの再発行時には、紛失カードの登録暗証番号の入力があつた場合だけ再発行を許可し、またカード情報登録時には、特定のカード発行機から発行されたカードに対してだけカード情報登録を許可し、

登録暗証番号の知らない者に対してカードが発行されないようにするとともに、特定のカード発行機以外のもので発行されたカードにはカード情報が登録されないようにして、不正カードの発行を防止するようにしたものである。

（以下余白）



以下この発明の実施例を図面を参照して説明する。

第１図はこの発明を適用した金融取引処理システムのブロック図である。

このシステムは、親機１、子機２、カード発行機４を通信回線で接続するオンラインシステムである。

子機２の制御装置の一例を示す計算機２０（以下CPU20という）には、メモリ２１、第１のバッファレジスタ２２、キーボード２３、支払機24、表示装置２５（以下CRT25という）、第２のバッファレジスタ２６がバス接続している。また、カードリーダ２７とバッファレジスタ２２がバス接続され、データはバッファレジスタ２２を介して、カードリーダ２７とCPU20との間で受け渡しされる。CPU20は、この他にカードリーダ27から線２８を介してカード入力の検知信号を受け、また警報機３０に対して線２９を介しアラーム信号を出す。

親機１は、その制御装置の一例を示す計算機10（以下CPU10という）と、口座番号に対応して残高、あるいは登録暗証番号や後述の発行禁止符号を記憶するメモリ１１と、バッファメモリ１２とを有し、この親機１と上記の子機２は、モデム１３，３１を介して通信回線５で接続され、子機２はオンラインで作動するようになつている。

また、親機１には通信回線６によつてカード発行機４がオンライン接続されている。このカード発行機４は、その制御装置の一例である計算機40（以下CPU40という）と、カード発行を行なうオペレータの番号等を記憶するメモリ４１と、口座番号やオペレータ番号を入力するキーボード４２と、表示装置４３（以下CRT43という）と、カードに口座番号を記録してカード発行するカードライタ４４と、バッファメモリ４５とを有し、モデム４６を介して通信回線６によつて親機１と接続されている。

第２図は子機２のキーボード２３のキー構成を示す。このキーボード２３は、０～９の数値キー230，ＣＬキー231，紛失キー232，強奪キー

233を有し、数値キー230は口座番号，暗証番号等を入力するときに使用され、ＣＬキー231は入力したキーを無効にするときに使用され、また紛失キー232はカードを紛失してカード再発行を要求するときに、確認キー233は紛失キー操作後に紛失を再度確認したときにそれぞれ使用される。

第３図は子機２のメモリ２１の部分マップ、第４図は親機１のバッファメモリ１２の部分マップ、第５図はカード発行機４のメモリ４１の部分マップをそれぞれ示す。また第６図(A)，(B)，(C)は子機２のCPU20の動作を示す制御フローチャート，第７図(A)，(B)は親機１のCPU10の動作を示す制御フローチャート，第８図は親機１のメモリ１１の部分マップ，第９図はカード発行機４のCPU40の動作を示す制御フローチャートを示す。

子機２の動作は第６図(A)のステップｎ１（以下ステップｎｉは単にｎｉという）からはじまる。

ｎ１は紛失キー232が操作されたかどうかをみる。操作されていなければｎ２へ進み、カード入力されているかどうかをチエックする。紛失キー232が操作されているとｎ1→ｎ3と進み「紛失確認」を指示する表示をおこない、その後ＣＬキー231が操作されると「カード挿入」を指示する表示をおこなつてｎ４へ進む。そしてｎ４で確認キー233が操作されれば第６図(C)のｎ56へ進み、操作されなければｎ１へ戻る。

ｎ２でカード入力を検知すると、ｎ５でカード読取りをおこなう。カードには発行時に口座番号だけが記録されている。したがつてこのｎ５で読取つた情報が口座番号だけであれば、そのカード使用は初回である。ｎ６はこの判定をおこなう。そして初回であれば第６図(B)のｎ７へ進む。

まずカード使用が初回であつて、且つそのカードがカード発行機４から発行された正式なカードである場合の制御手順を説明する。

第６図(B)に示す制御手順では、カードへのカード情報登録をおこなう。なお、この実施例では、カード情報を、質問とその質問に対する答と暗証番号とで構成している。このようにカード情報に暗証番号の他、質問とその質問に対する答を含ませることによつて、暗証番号の桁数を大きくすることなく個人照合の精度を高めることができ、また暗証番号の桁数を大きくしない分だけカード情報が記憶しやすくなるという利点がある。

カード情報を登録するための最初のステップｎ７では、読取つた情報（口座番号）を領域ＭＡにセットする。この領域ＭＡは領域MA1～MA8で構成される。領域MA1～MA8は、順に口座番号，暗証番号，第１の質問の番号，第１の質問の答，第２の質問の番号，第２の質問の答，第３の質問の番号，第３の質問の答，を記憶するために利用される。次にｎ８で「暗証番号入力」を指示する表示し、ｎ９，ｎ10で入力された暗証番号を領域ＭＡ２にセットする。暗証番号を領域ＭＡ２にセットすると、次いでｎ11で「質問ＮＯ．入力」を指示する表示をし、ｎ12，ｎ13で入力された質問ＮＯ．を領域ＭＡ３にセットする。ｎ14では、領域ＭＡ３にセットされたデータ（第１の質問NO.）を参照して、質問と答の選択枝とのファイルを記憶している領域ＭＱから質問内容データ（質問と答の選択枝を読み出して表示する。そしてｎ15で、操作者（カード所有者）が入力したデータ（選択した答）を領域ＭＡ４にセットする。以上のｎ11～ｎ15までで第１の質問とそれに対する答のセットを完了する。同様にして、ｎ16～ｎ20で第２の質問とそれに対する答のセットをおこない、ｎ21～ｎ25で第３の質問とそれに対する答のセットをおこなう。

なお上記のファイルは予め領域ＭＱに記憶されていて、ｎ12，ｎ17，ｎ22で入力する質問ＮＯ．は操作者がそのファイルの中から自由に選択できるようになつている。またこの実施例では入力する質問の数を３個としたが、質問数は上記ファイルに設定される質問数以下であるならば任意の数に設定出来る。こうして、暗証番号，三つの質問とそれらに対する答とからなるカード情報を領域ＭＡにセットすると、次にこのカード情報をカードに登録していいかどうかを親機１に問い合わせる。ｎ26はこの問い合わせのために，登録メッセージと、口座番号と、暗証番号とを親機１に送信

するステップである。

第7図(A)において、親機1はn100で通信回線から受信したデータを、バッファメモリ12の領域BM1～4にセットする。領域BM1はメッセージを、領域BM2は口座番号を、領域BM3は暗証番号またはオペレータ番号を、領域BM4は支払要求金額をそれぞれセットするためのものであるが、この段階では領域BM1～BM3にそれぞれ登録メッセージ，口座番号，暗証番号がセットされ、他の領域は空白である。n101～n104（第7図(B)も参照）は領域BM1にセットされているメッセージの内容をみるステップであり、支払メッセージであればn101→n105 紛失メッセージであればn102→n112，登録メッセージであればn103→n117，発行メッセージであればn104→n124，その他であればn104→n132と進む。

今、領域BM1にセットされているメッセージは登録メッセージであるため、n103→n117と進み、n117で領域BM2の口座番号にもとづいてその口座番号に対応するカード管理情報を、メモリ11からバッファメモリ12の領域BM5～BM8に読出してセットする。このカード管理情報は、第8図に示すように、口座番号に対応して、登録された暗証番号，残高，カードの発行禁止の場合は発行禁止符号，カード情報の登録禁止の場合は登録禁止符号，および発行者オペレータ番号の情報で構成される。したがってn117では、領域BM5～BM8に順に、登録暗証番号記憶領域MR1，残高記憶領域MR2，発行禁止符号記憶領域MR3，登録禁止符号記憶領域MR4のそれぞれに記憶されているデータが転送される。

後述するように、上記のカード管理情報のうち登録禁止符号は、カード発行機4から発行された正式なカードの初回使用時に限りリセットされている。このため、n117→n118→n119と進み、n119でバッファメモリ12の領域BM1にOKメッセージがセットされる。こうして登録を許可する旨のOKメッセージを領域BM1にセットすると、次いでn120で領域BM3の暗証番号（カード所有者が入力した暗証番号）をスクランブルして領域BM5へ、登録暗証番号としてセットする。また、n121で領域BM8に登録禁止符号をセットし、後述するように以後のカード情報の登録が禁止されるようにしてから、n122で領域BM5～BM8のセットデータを、領域BM2の口座番号に対して割付けられたメモリ11の領域に格納する。なお、n120でのスクランブルは、たとえば口座番号の下4桁に暗証番号を加算する方法（けた上げ分は無視）を用いる。このように登録暗証番号をスクランブルしたカード管理情報にすることによって他人によってメモリ11から登録暗証番号を直接読み出される恐れがなくなる。

以上の処理を終えるとn110（第7図(A)）へ進み、領域BM1のセットデータ（OKメッセージ）を子機2に送信する。カード発行機4で正式に発行されたカードの初回使用時の場合は、以上で親機1の手順が終了する。なお、n118で登録禁止符号がセットされていると（このような状態は、後述するように偽造カードを登録しようとする場合に起こる），n123で不正メッセージが領域BM1にセットされ、n110でこの不正メッセージが子機2に対して送信される。

子機2は、n27（第6図(B)で受信待ち状態にあるが、上記の手順で親機から登録に対するメッセージが送信されてくると、n28でそのメッセージを判定する。このメッセージはOKメッセージ（n119）か不正メッセージ（n123）である。そしてOKメッセージならn29へ進み、不正メッセージならn64（第6図A）へ進む。

OKメッセージは登録を許可するメッセージであるから、n8～n25で領域MAにセットしたカード情報をカードに記録しなければならない。n29，n30はこのカード情報を記録するステップである。なお、n29において正しいカード情報をスクランブルしているが、このスクランブルはカードの盗難時などに、正しいカード情報が他人に解読されないようにするための処理である。ここでのスクランブルは、この実施例では正しいカード情報の9の補数をとる方法でおこなわれる。こうしてカード情報の登録（カードへの記録）が終了すると、

n31（第6図(c)）へ進んでカードを返却し、さらにn32でカードが抜取られるのを確認すると、n33へ進んでカード挿入」を表示して次のカードの挿入を待つ。

一方、n28で受　メッセージを不正メッセージと判定すると、n64へ進み、警報機30で　報する。そして警報機30の動作後は、係員が不正使用客に対応し、機械のリセットボタンを押した(n65)後、n31へ進んでカードの返却をおこなう。

以上のようにして、カードの初回使用時には、そのカードがカード発行機4で正式に発行されたカードであれば、つまり登録禁止符号がセットされていなければ、操作者（カード所有者）の指定したカード情報が登録され、そのカードがカード発行機4以外のもので発行された偽造カードであれば、つまり登録禁止符号がセットされていれば、警報機が動作することになる。

次にカード情報の登録が終了して、カード使用が2回目以降である場合の制御手順を説明する。

この2回目以降のカード使用については、カードが正しい所有者によつて使用されたものでるかどうかをチエックする個人照合がおこなわれる。

まず、カード入力を検知してから（第6図(a)，n2）磁気読取りをおこなう(n5)。この場合カード自身には、口座番号と、暗証番号，質問および答（3種類）のカード情報とが記録されている。n5を終えるとn6→n34と進む。

n34では、n5で読取つたカード情報をスクランブル解読し、解読後の情報をメモリ21の領域MAに書き込む。この場合のスクランブルはn29のスクランブルと対応して、その補数でおこなわれる。n35ではCRT25に「暗証番号入力」を指示する表示をする。n36，n37はキーボード23から入力された所定の桁数の数字を領域MBに書き込む。n38はその領域MBの記憶データと領域MA2の記憶データ（カードに登録された暗証番号）との一致チエックをする。一致すれば、暗証番号が正しく入力されたことになるからn39へ進む。

n39～n47は質問に対する答のチエックをおこなうステップである。

まずn39では、領域MA3の内容をインデックスにしてファイル（領域MQ）の中から、そのインデックスに対応する質問内容データ（質問と答の選択枝とから構成される）を読出して表示する。この例では、領域MA3の内容が質問NO．3であるから、対応する領域MQ3の内容が表示される。なお、上述したように質問と答の選択枝ファイルは予め作成されてメモリ21内に格納されている。続いてn40で、キーボード23から入力された答のデータを領域MBに書込む。n41では領域MBに記憶された答と、領域MA4の答（登録されている答）とを比較する。この二つの答が一致すれば、次のチエックをおこなう。次の質問の表示およびその答のチエックは、n42～n44でおこなわれる。チエックの仕方はn39～n41と同じである。つまり、n42で次の質問と答の選択枝を表示し、その質問に対して入力されて領域MBに記憶された答と領域MA6の答とを比較してその一致をチエックする。同様にして、n45～n47でも3番目の質問に対する答のチエックをおこなう。なお、前述したように、この例では、質問数を3個としているが3個に限られない。カードへの質問と答の登録の際、質問ファイルのすべての質問の中から定められた数（ここでは3個）の質問を選ぶようにしてある。

n47のチエックで答が一致すれば、n48以下の金銭の支払処理に移る。しかし、上記の3個の質問の答が一つでも一致しなければ，n41若しくはn44またはn47からn64へと進み警報機30を作動させる。また、n38で暗証番号が一致しなくてもn64へ進んで警報機30を作動させる。このようにして、質問に対して入力した答が、登録してある答と異なれば、そのカード使用を無効にすることができる。警報機30の動作後は、係員が不正使用客に対し、機械のリセットボタンを押す(n65)。リセットボタンの操作信号を検出するとn31へ進む。

次にn48以下の手順について説明する。

n48は「金額入力」を指示する表示をする。

n49,n50はキーボード２３から入力された支払要求金額を、領域ＭＢにセットする。支払要求金額は残高以下でなければならないが、残高データは親機のメモリ１１にカード管理情報として記憶されているため、この領域ＭＢにセットされたデータ（支払要求金額）は、支払いしていいかどうかをチエックするために支払メッセージ，口座番号とともにn51で親機１へ送信される。

第７図(A)において、親機１は子機２からの送信データを受信すると、その受信データを領域BM1～ＢＭ４にセットする（n100）。この段階で領域ＢＭ１のメッセージ領域には支払メッセージが、領域ＢＭ２にはカードの口座番号が、領域ＢＭ３には暗証番号が、領域ＢＭ４にはn49で領域ＭＢにセットされた支払要求金額がセットされる。そしてn101で領域がＢＭ１のメッセージをチエックし、そのメッセージが支払であるならn105へ進む。上記メッセージは、今、支払メッセージであるから、n101→n105へと進む。n105では、領域ＢＭ２にセットされた口座番号を参照してその口座番号に対応するカード管理情報をメモリ11から読み出すとともに、領域ＢＭ５～ＢＭ８にセットする。n106でこの情報のうち領域ＢＭ８にセットされた残高と、領域ＢＭ４にセットされている支払要求金額との比較をおこない、前者が後者よりも小さい場合を除き、支払いをＯＫするＯＫメッセージを領域ＢＭ１にセットする(n107)。n108,n109はカード管理情報の書き換え手順である。n108では元の残高から支払要求金額を差引いた額の金額データが領域ＢＭ６にセットされる。次いでn109では領域ＢＭ２の口座番号を参照して、領域ＢＭ５～ＢＭ８のデータをメモリ11のカード管理情報記憶部に書き込む。以上の処理を終えた後、n110でで領域ＢＭ１のメッセージ、つまりＯＫメッセージを子機２に対して送信する。

一方、n106で領域ＢＭ６のデータ（残高）が領域ＢＭ４のデータ（支払要求金額）より小さければ、つまり支払要求金額が残高を越えていれば、n111へ進んで、残不足メッセージを領域ＢＭ１にセットする。この場合はカード管理情報のうち残高データの書き換えをおこなうことなくn110へ進み、ここで領域ＢＭ１にセットされている残不足メッセージを子機２に対して送信することになる。

以上のようにして親機１での処理が終わり、子機に対してＯＫメッセージまたは残不足メッセージが送信されると、子機はn52（第６図(A)）でそのメッセージを受信する。そしてn53でそのメッセージを解読し、ＯＫメッセージであればn54へ、残不足メッセージであればn55へ進む。前者の場合、すなわちＯＫメッセージである場合は、n54で領域ＭＢのセットデータ（支払要求金額）を支払機２４に転送し、領域ＭＢにセットされている支払要求金額の支払いを支払機２４に指令する。支払いを済ませると、前述したn31以下の手順によつて、カードの返却処理をおこなう。

一方、n53で受信データが残不足メッセージと判定された場合はn55へと進み、支払機５を動作させることなく「残不足」表示をおこなう。そしてn31以下のカード返却処理を実行して終了する。

以上の手順で、カード使用の際のチエックと、そのチエックがＯＫである場合の預金支払いをおこなうことができる。

次に、カードを紛失したため、そのカードを再発行する場合の制御手順を説明する。

この場合には、まず紛失したカードの所有者が、キーボード２３の紛失キー232を操作する。第６図(A)において、この紛失キー232が操作されると、n1→n3と進み、さらに紛失を確認した後確認キー233が操作されると（n4）、n56（第６図(B)）へ進む。

n56では、カード再発行準備のために「口座番号入力」を指示する表示をする。次いで、n57，n58で、キーボード２３から入力された紛失カードの口座番号が領域ＭＡ１にセットされる。この口座番号のセットを完了すると、次にn59で個人照合のために、紛失カードの「暗証番号入力」を指示する表示をする。そしてn60,n61で、キーボード２３から入力された暗証番号を領域ＭＡ２にセットし、さらにこの暗証番号が正しいかどうか

チェックするために、この暗証番号を口座番号と紛失メッセージとともに親機1へ送信する。子機2は以上の処理を終えて、n63で「カード挿入」表示をして通常のカード入力待ち状態に戻る。

親機1は、上記の手順によつて送信されたデータをn100で受信して、領域BM1に紛失メッセージを、領域BM2に口座番号を、領域BM3に暗証番号をセットする。次に領域BM1のメッセージが紛失メッセージであるから、n102→n112へと進む。n112では、前述のn105と同様に、領域BM2の口座番号を参照してその口座番号に対応するカード管理情報を読出して、領域BM5～BM8にセットする。さらに、n113で、領域BM5にセットされた登録暗証番号のスクランブル値（n120で登録暗証番号はスクランブルされている）をスクランブル解読して領域BM5へ再セットする。このスクランブルは、n120に対応して口座番号下4桁をスクランブル値から減算することによつておこなう（ボローは無視）。次いで、n114で領域BM5の登録暗証番号と、領域BM3の入力暗証番号との比較をおこない、一致すればn115へ進み、不一致であれば親機1での処理を終了する。登録暗証番号が入力暗証番号に一致する場合には、n115で、領域BM7の発行禁止符号をリセットする。そしてn116でカード管理情報をメモリ11に再格納して処理を終える。

以上の手順によつて、暗証番号が正しく入力されれば、カード管理情報の発行禁止符号をリセットして、カードの再発行を可能にする。すなわち、発行禁止符号がリセットされたときだけ、後述するようにカード発行機4でのカードの発行が出来るようになる。したがつて、カードが紛失して再発行するためには、実際の再発行に先立つて紛失キーの入力と正しい暗証番号の入力が必要となつてくる訳である。

次にカード発行機4のCPU40の制御手順を第9図のフローチャートを参照して説明する。

n200,n201は、カード発行機4を操作するオペレータ番号を、メモリ41の領域MEにセットするステップである。このオペレータ番号はオペレータ自身がキーボード42から入力する。メモリ41には、第5図に示すように、領域MOに予めオペレータ番号1～nが登録されていて、この登録オペレータ以外は発行機の操作を許可されない。n102ではこのオペレータのチエックをおこなう。すなわち、領域MEにセットされたオペレータ番号が領域MOに登録されているオペレータ番号1～nの中にあれば、操作を許可することとしてn202→n203と進み、そうでなければn202→n212と進む。n203では、「口座番号入力」の指示を表示する。n204,n205では、入力された口座番号を領域M.Dにセットする。なお、オペレータはカード発行に際し、その発行するカードの口座番号を知つているものとする。以上の処理の後、n206で発行メッセージを領域MCにセットし、続いてn207で領域MC～MEのデータ、すなわち発行メッセージ，口座番号，オペレータ番号を親機1に送信する。

親機1は、上記のデータをn100で受信すると、領域BM1に発行メッセージを、領域BM2に口座番号を、領域BM3にオペレータ番号をセットする。そして領域BM1に発行メッセージがセットされているから、n104→n124と進む。n124では、n105,n112,n117と同様に、口座番号に対応するカード管理情報をメモリ11から読出して領域BM5～BM8にセットする。次にn125で、領域BM7に発行禁止符号がセットされているかどうかをみる。もしセットされていればn131へ進み、セットされていなければn126へ進む。n126へ進む場合、つまり発行禁止符号がリセットされている場合は、カード発行を許可し、n131へ進む場合、つまり発行禁止符号がセットされている場合はカード発行を許可しないことになる。n126では、カード発行の許可をするため領域BM1に発行可のメッセージをセットする。反対にn131ではカード発行を許可しないために、領域BM1に発行不可のメッセージをセットする。前者の場合、すなわちn125→n126と進む場合は、n127で領域BM8の登録禁止符号をリセットす

る。このn127は、新たに発行されるカードに対し、その初回使用時にカード情報が登録されるようにするためのステップである。（n118参照）。続いてn126で領域BM7へ発行禁止符号をセットして、今発行しようとしているカードとは別のカードが発行されるのを禁止する。n129では、領域BM3にセットされているオペレータ番号を領域9にセットする。そしてn130で口座番号に対応するカード管理情報をメモリ11に格納する。以上の手順で、n130で格納されたカード管理情報には、発行禁止符号がセットされており、また登録禁止符号はリセットされており、さらに新たにカード発行をおこなおうとしているオペレータ番号が含まれている。

n126～n130の処理、またはn131の処理を終えると、n110へ進み、領域BM1にセットされているメッセージをカード発行機4に対して送信する。

カード発行機4は、n208で上記のメッセージを受信する。そしてそのメッセージが発行可のメッセージならn209→n210と進み、領域MDにセットされている口座　号をカードライタ44に転送し、その番号のカードへの記録を指示するとともにn211でカードを発行する。また発行不可のメッセージならn209→n212と進み、警報をおこなう。n213で、係員がカード発行者に返却し、警報がリセットされるとカード発行機での処理が終わる。

このようにしてカード発行をする際は、発行しようとするカードの口座番号に対応するカード管理情報、およびオペレータ番号がチェックされ、発行禁止符号がセットされていなくて、且つオペレータ番号が登録オペレータ番号である場合にだけ、カード発行がおこなわれる。

以上のように、この実施例では、カードの発行を禁止するときに発行禁止符号をセットし、カード情報の登録を禁止するときに登録禁止符号をセットするようにしている。すなわち、発行禁止符号のセットはカードを発行するときにおこない、登録禁止符号のセットはカード情報の登録時におこなうようにしている。一方、発行禁止符号のリセットは紛失キーが操作され、しかも紛失カードの正しい暗証番号が入力されたときにおこない、また登録禁止符号のリセットは、カード発行機がカードを発行するときにおこなうようにしている。

したがつて、カードを一度発行すると、発行禁止がかかつて以後同じ口座番号のカード（偽造カード）が発行できなくなり、また、親機1とオンライン接続される所定のカード発行機以外の発行機で偽造カードが発行されると、そのカードの初回使用時には登録禁止がかかつているから登録ができなくなる。それ故、カードの発行段階および初回使用時段階において不正な偽造カードの作成を防止することができる。

（以下余白）

以上のように、この発明によれば、カードの再発行の条件としてその紛失カードに登録しておいた暗証番号の入力設定が必要であるため、その暗証番号を知らない第3者に対する同一口座番号のカード（不正カード）発行を完全に防止することができる。また、カード情報の登録の条件としてそのカードが特定のカード発行機で発行されたものであることが必要であるため、全く無関係のカード発行機で発行されたカードはその登録（初回使用）の段階で不正カードとみなされる。したがつて、カードの発行段階と登録段階とで不正なカードの作成されることが防止され、通常時において使用できるような不正カードの発行される可能性を殆んど無くすことができるため、カードを媒体とする取引等の安全性を非常に高くすることができる。

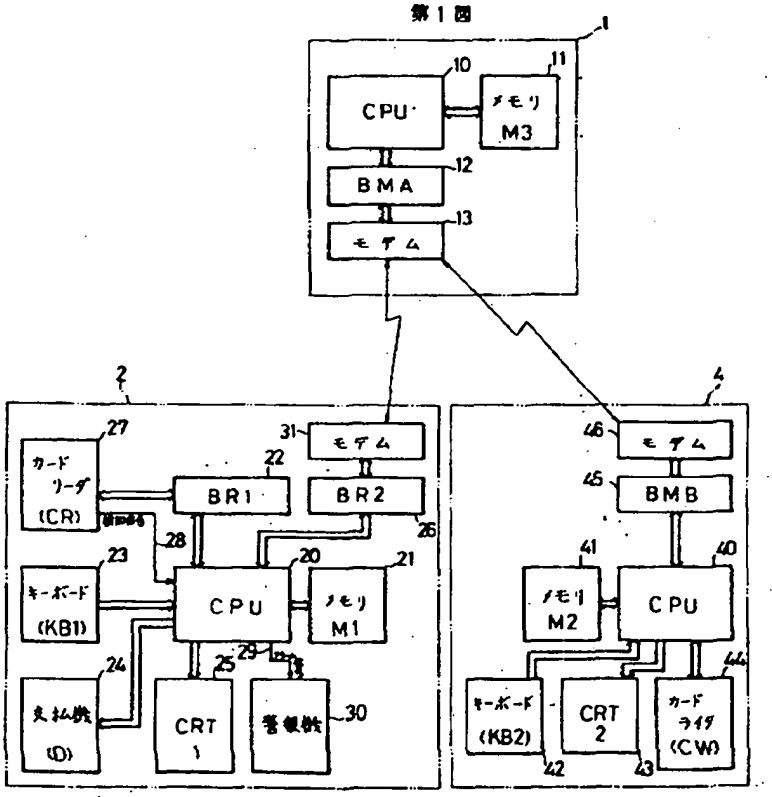
4.図面の簡単な説明

第1図はこの発明を適用した金融取引処理システムのブロック図、第2図は子機のキーボードのキー構成図、第3図は子機のメモリの部分マップ、

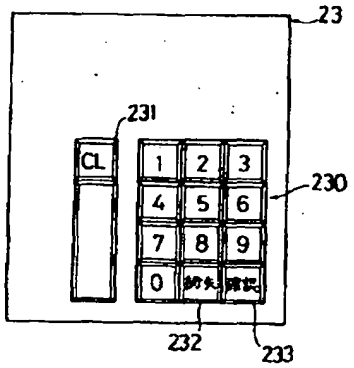
第4図は親機のバッファメモリの部分マップ、第5図はカード発行機のメモリの部分マップ、第6図(A)～(C)は子機の計算機の制御フローチャート、第7図(A)，(B)は親機の計算機の制御フローチャート、第8図は親機のメモリの部分マップ、第9図はカード発行機の計算機の制御フローチャートである。

出願人　立石電機株式会社
代理人　弁理士　小森久夫

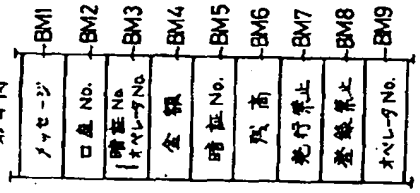
第1図



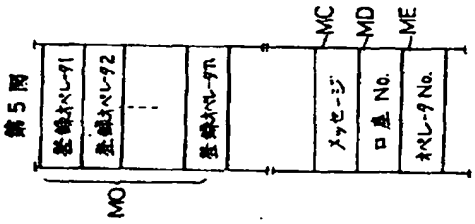
第2図



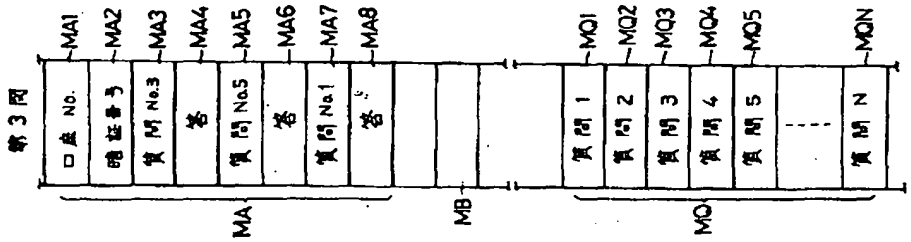
第4図



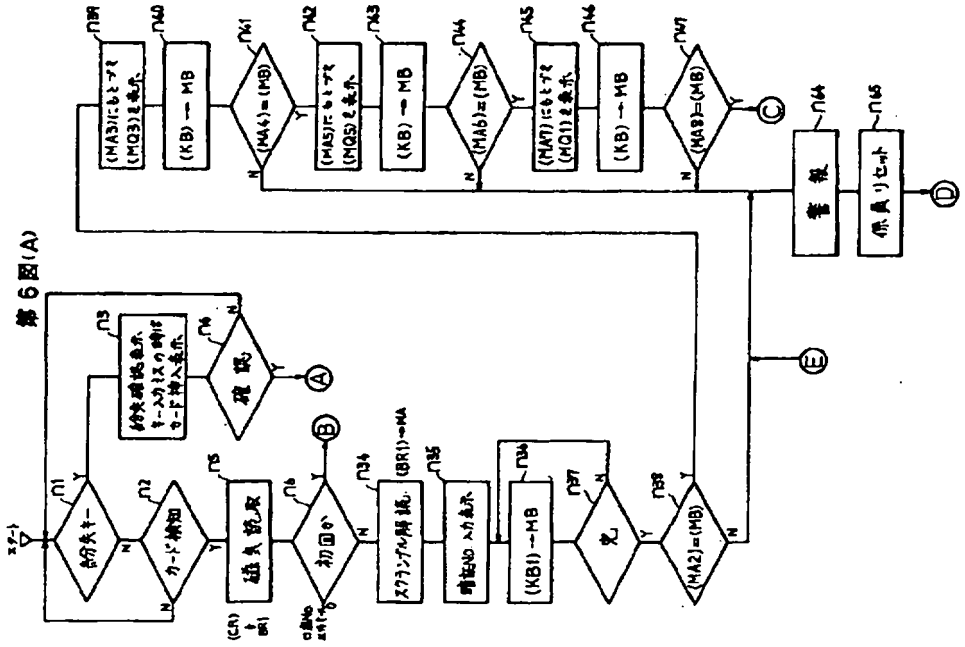
第5図



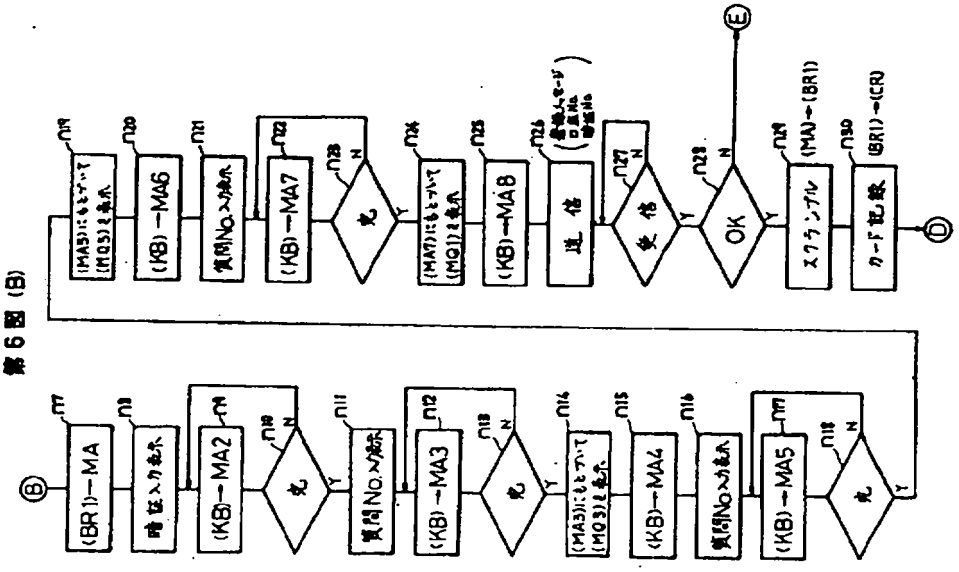
第3図



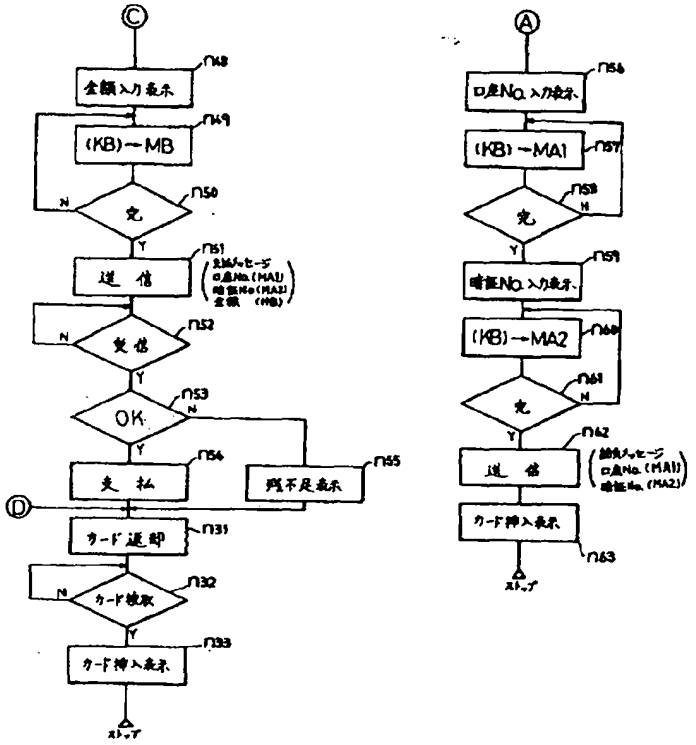
第6図(A)



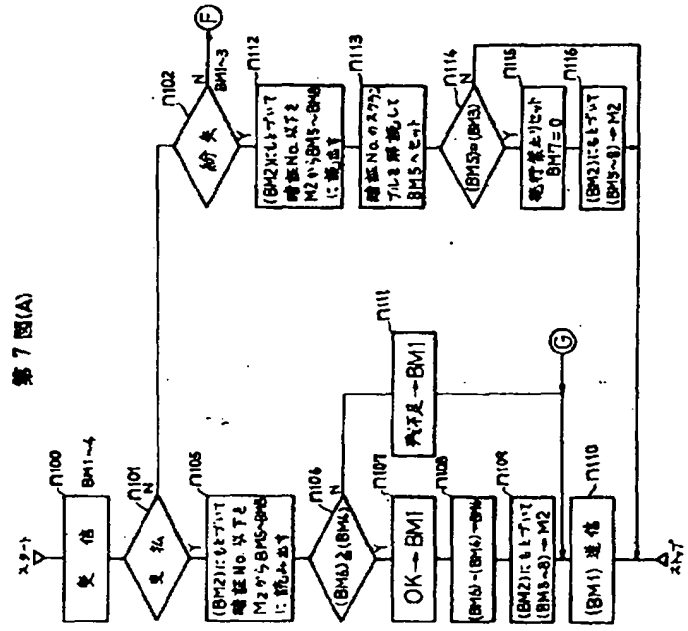
第6図(B)



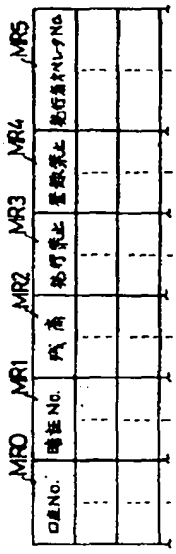
第6図(C)



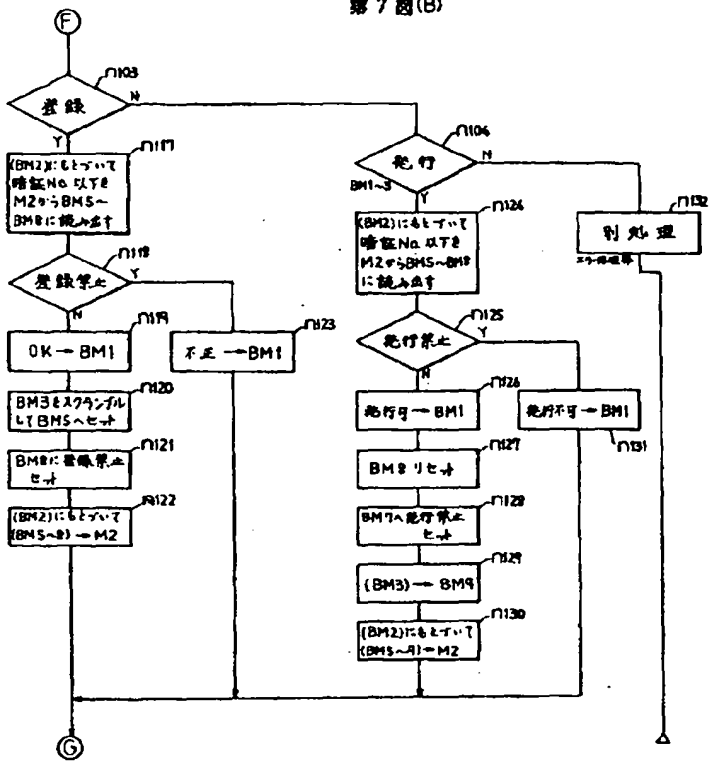
第7図(A)



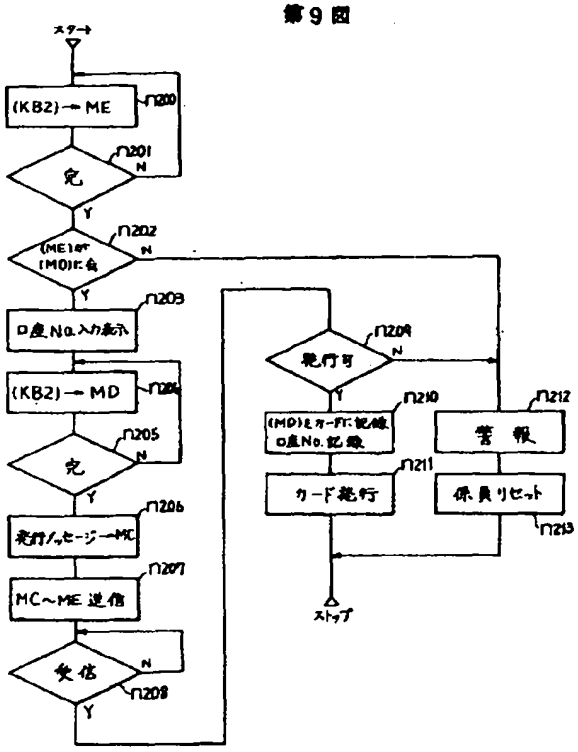
第8図



第7図(B)


Ⓕ
登録
N
Y
(BM2)にもとづいて暗証No.以下をM2からBMS～BM8に読み出す
登録禁止
Y
N
OK→BM1
不正→BM1
BM3をスクランブルしてBMSへセット
BM8に登録禁止セット
(BM2)にもとづいて(BMS～8)→M2
Ⓖ
発行
BM1～3
(BM2)にもとづいて暗証No.以下をM2からBMS～BM8に読み出す
発行禁止
発行可→BM1
発行不可→BM1
BM8リセット
BM7へ発行禁止セット
(BM3)→BM9
(BM2)にもとづいて(BMS～8)→M2
別処理

第9図


スタート
(KB2)→ME
完
(ME1)が(M0)に会
口座No.入力表示
(KB2)→MD
完
発行メッセージ→MC
MC～ME通信
受信
発行可
(MD)とカードに記録口座No.記録
カード発行
警報
係員リセット
ストップ

PAT-NO: JP358109970A

DOCUMENT-IDENTIFIER: JP 58109970 A

TITLE: PREVENTING METHOD FOR ISSUE OF INCORRECT CARD

PUBN-DATE: June 30, 1983

INVENTOR-INFORMATION:
NAME
ENDO, KOICHI

ASSIGNEE-INFORMATION:
NAME COUNTRY
OMRON TATEISI ELECTRONICS CO N/A

APPL-NO: JP56215538

APPL-DATE: December 23, 1981

INT-CL (IPC): G06F015/30, G07D009/00 , G07F007/08

US-CL-CURRENT: 235/380

ABSTRACT:

PURPOSE: To prevent the issue of incorrect card to the another person, by resetting a card issue inhibiting code only when the registrated secret number of a missing card is inputted at the re-issue of the card in a financial transaction processing system, and permitting the re-issue for the case.

CONSTITUTION: At the issue of a card, an account number, a registrated secret number, a balance, and at the inhibition of card issue, an issue inhibiting code, and at the inhibition of registration of

card information, an
card management information of a registration inhibiting code and an operator
number, etc. are transmitted from a slave device 2 to a master device 1, the
information is cheked by using a memory 11 of the master device 1. The
registration inhibiting code in the information is reset only at the initial
input of the normal card issued from a card issue machine 4, then the message
of registration permission is transmitted to the slave device, and a
registration inhibiting code is set to inhibit the further registration. The
slave set makes registration with the message. If the card is missing and
re-issued, the secret number is compared with the registrated secret number,
and when they are coincident, the registration inhibiting code is reset and the
re-issue is permitted.